Multiparty Communication Models and Applications

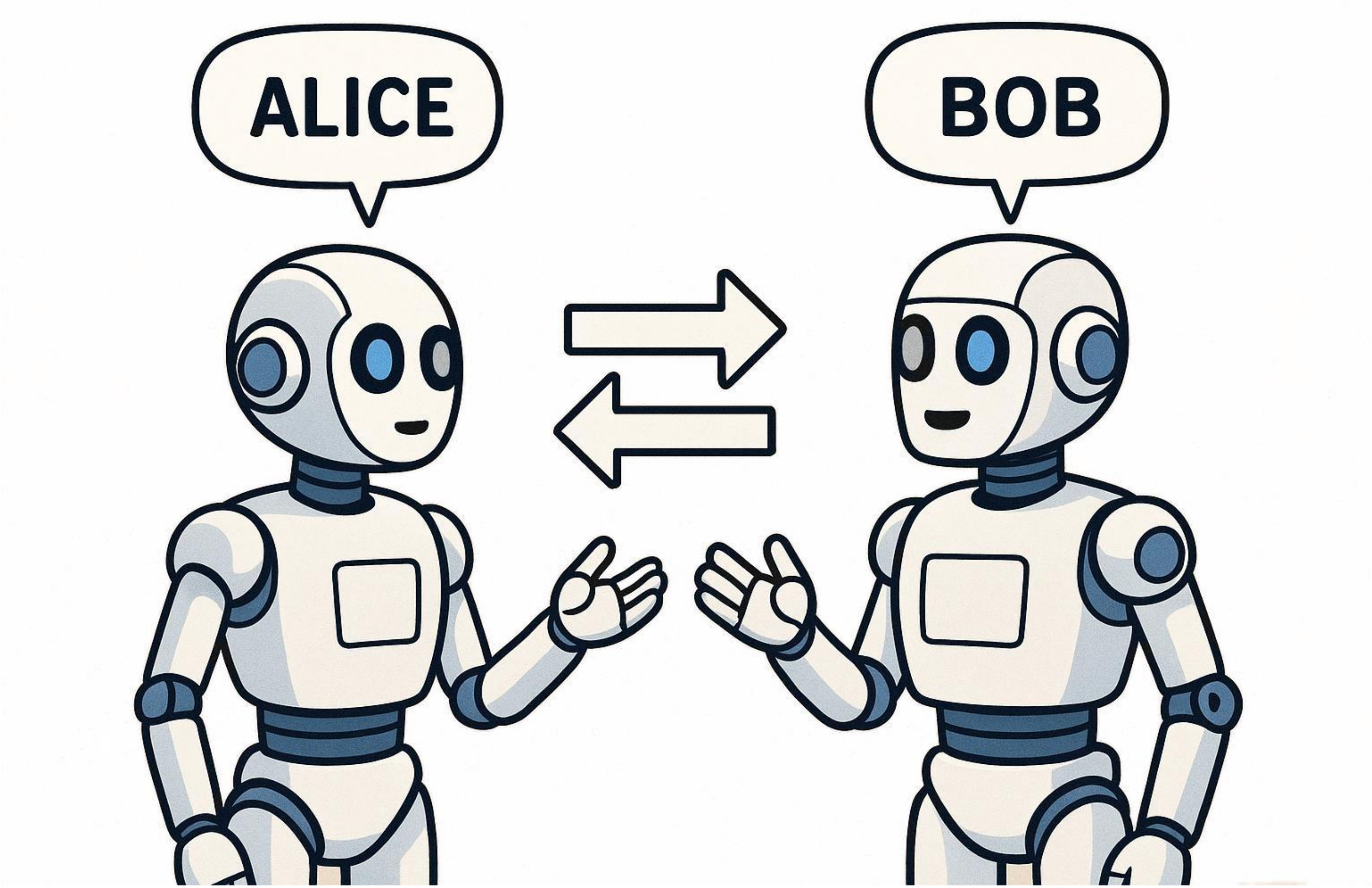
Speaker: Xianbin Zhu (under the supervision of Jara Uitto)

Outline

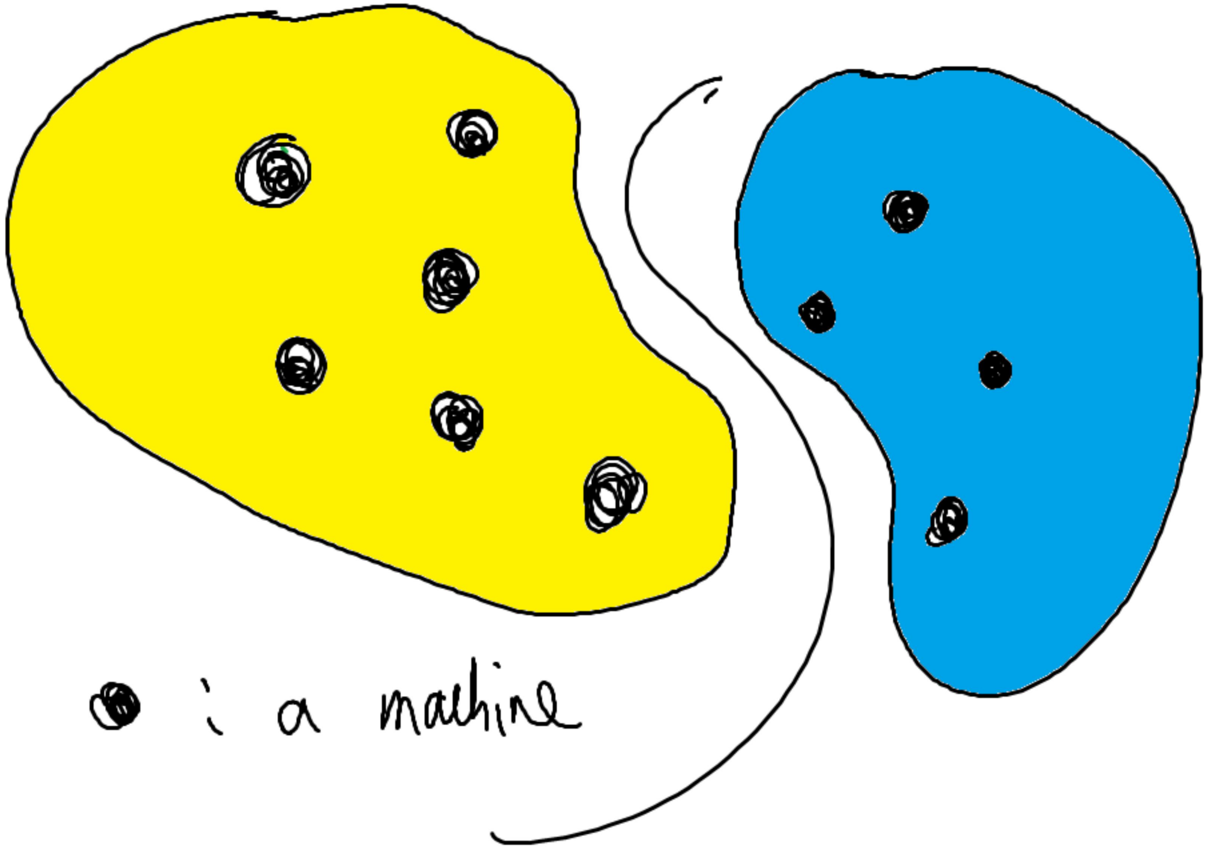
- 1. Motivation
- 2. Models
- 3. Applications: distributed computing, streaming algorithms, crypotography

Motivation

Two-party communiation model

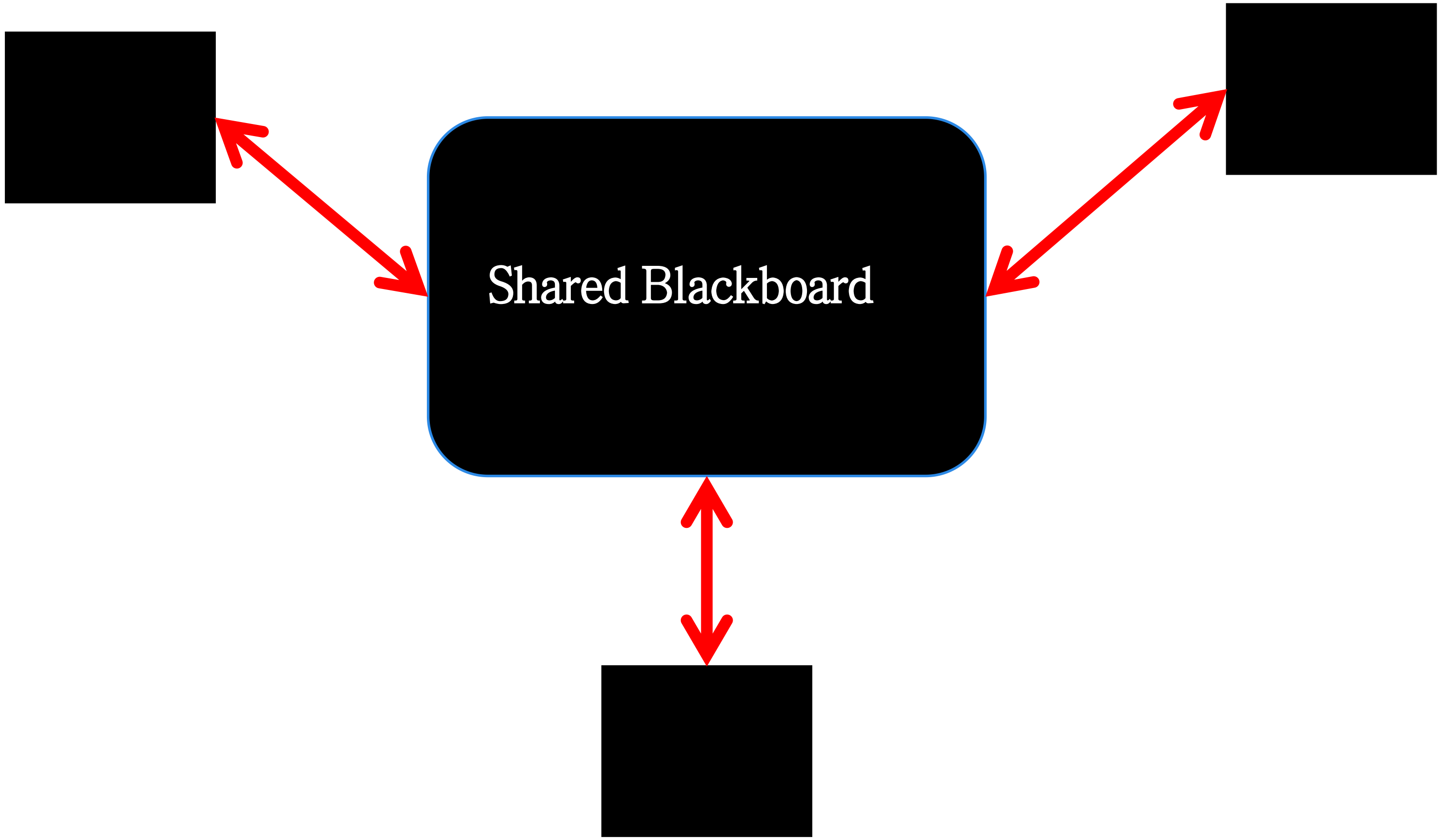


Two-party communication model in Distributed Computing

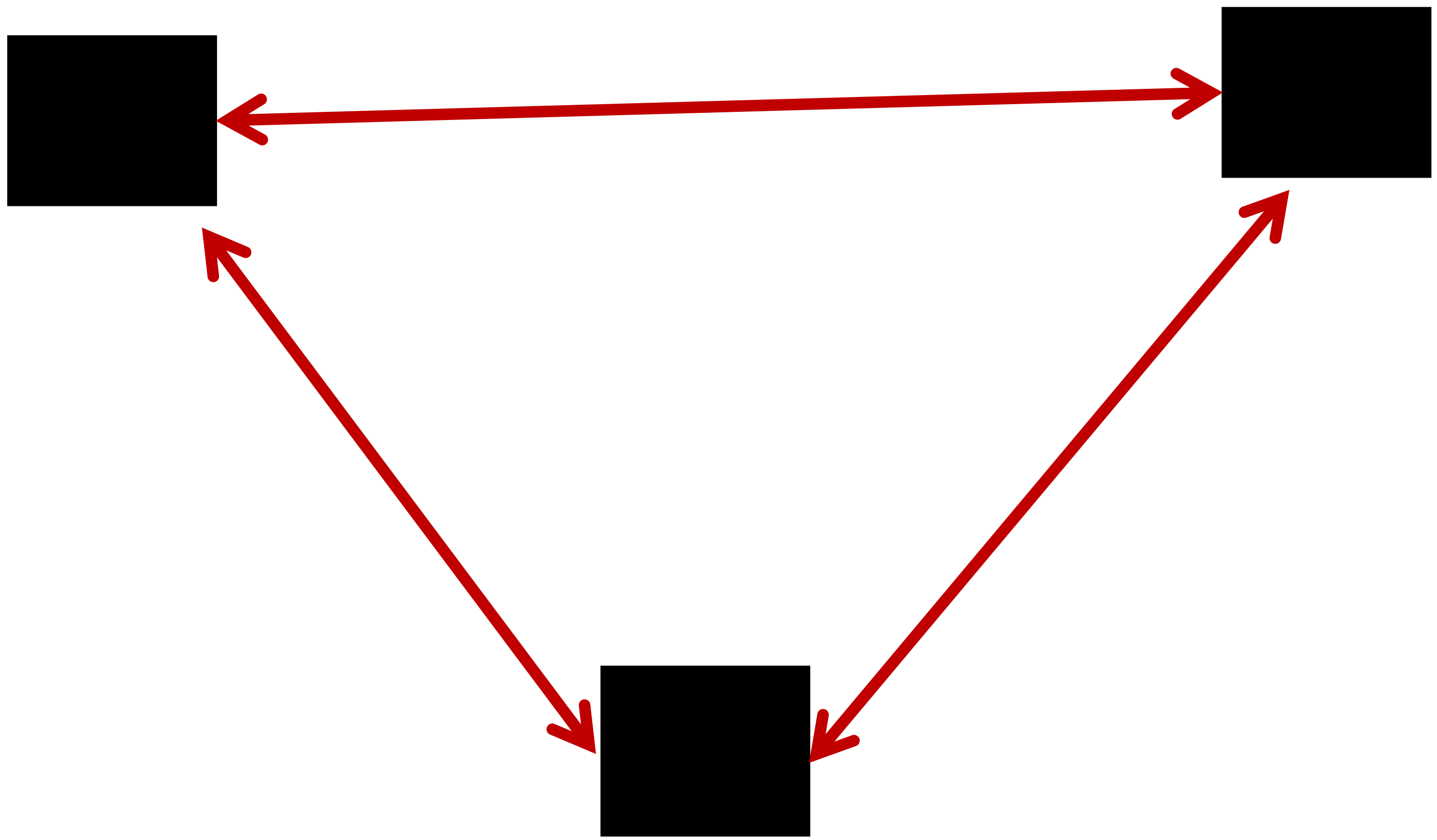


Multiparty Communication Models

Multiparty Communication Models



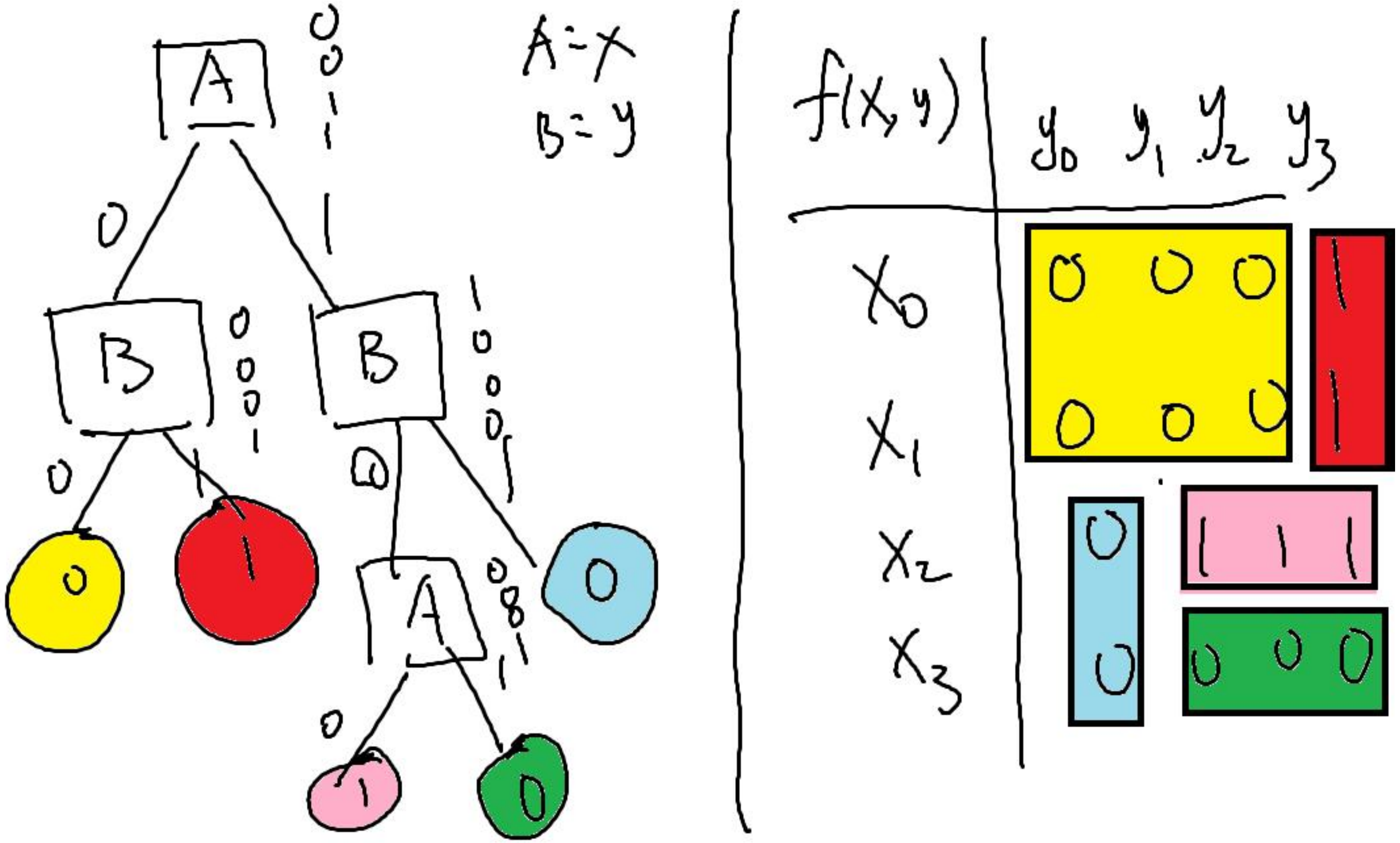
message passing model (without shared blackboard)



Tools for multiparty communication models

- n-dimensional box
- Information theory
  1. Entropy
  2. Mutual Information
- Round Elimination
- (open) New Tools

Combinatorial Rectangle



n-dimensional Box

Information Theory (Some)

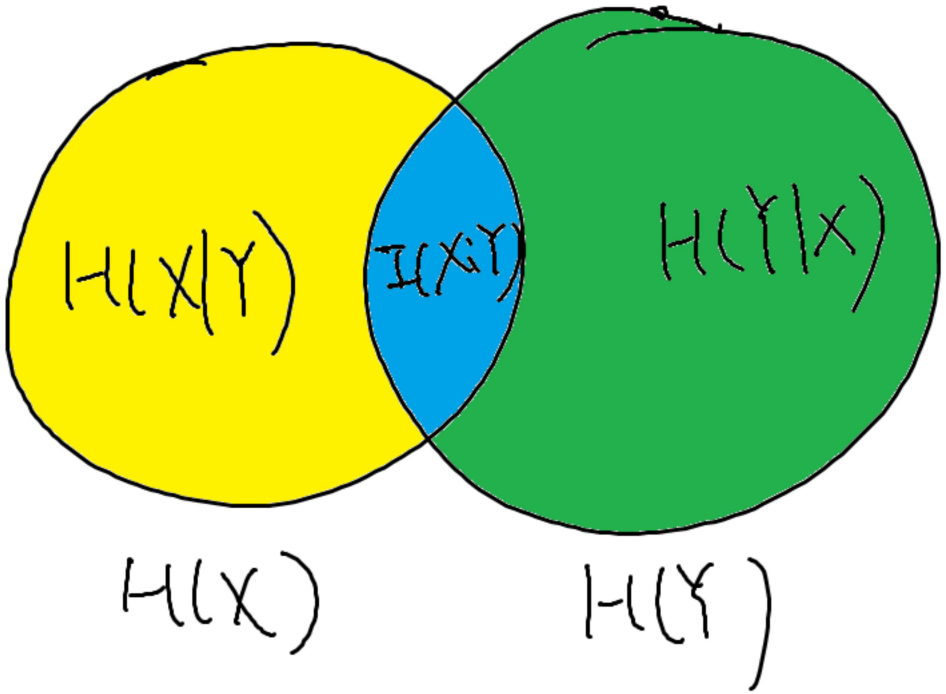
$$H(X) = -\sum_{x \in \mathcal{X}} p(x) \log p(x)$$

For two random variables X and Y:

$$I(X;Y) = \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} p(x,y) \log \frac{p(x,y)}{p(x)p(y)}$$

$$I(X;Y) = H(X) + H(Y) - H(X,Y)$$

The Relationship bewteen Entropy and Mutal Information



Why Information Theory Works

- $CC(f) \geq |\pi| \geq H(\pi) \geq I(\pi : XY) = IC(f)$

- Under some distributions, mutual information has nice properties, e.g., Decomposition Lemma
- Information Complexity has a nice direct sum property

Applications

1. Lower Bounds in Distributed Computing

- **Distributed Sketching Model**

I. A referee and n nodes.

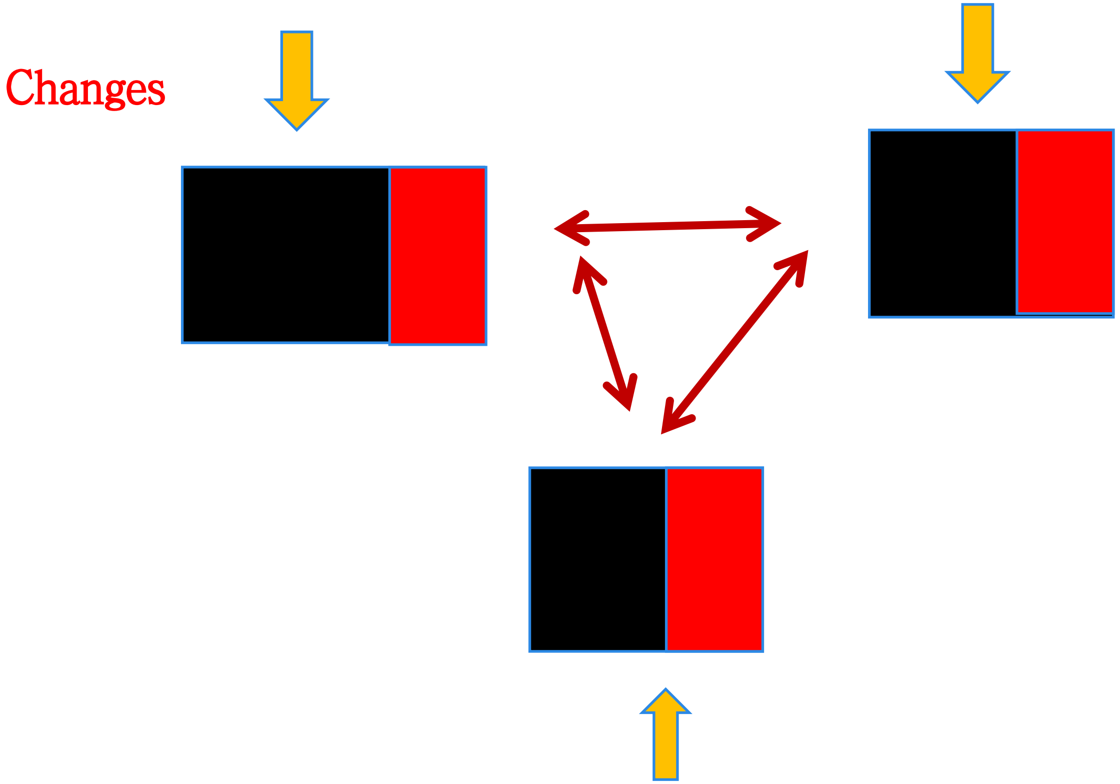
II. Each node knows its neighbors.

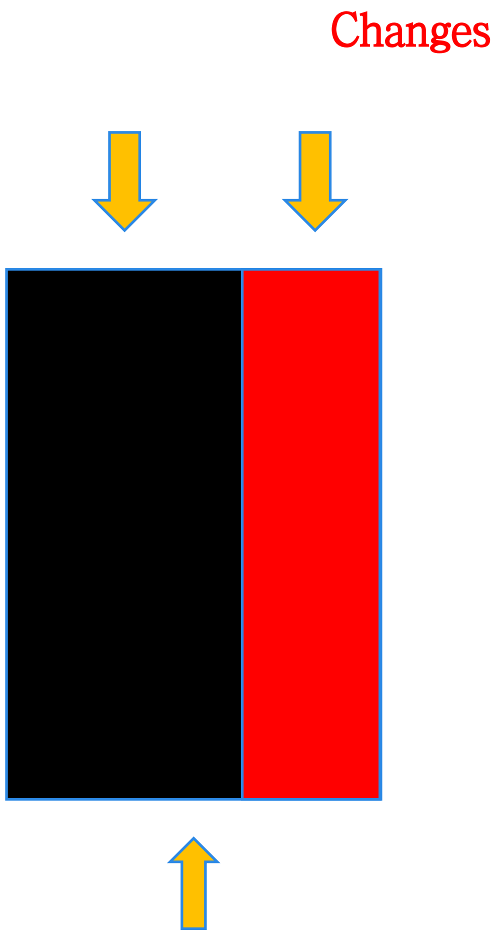
III. Initially, the referee has **nothing**. After receiving messages from nodes, this referee outputs the result (**one-round**).

Result: Any public-coin distributed sketcihng protocol for MM(MIS) with constant successful probability requires $\Omega(n^{1/2-\varepsilon})$ sketch(a message sent by each node). [PODC2020]

Open: Dynamic Distributed Algorithms

- Distributed Data Structure





Open: Dynamic Distributed Algorithms

1. Lower Bounds?

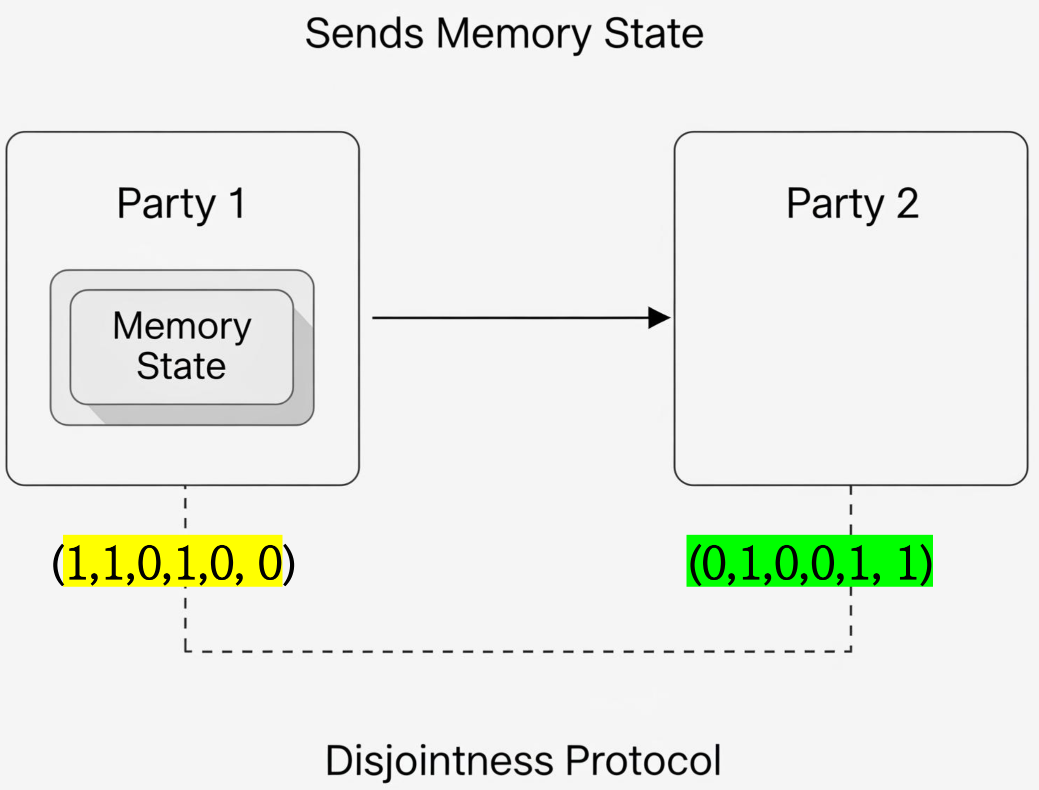
2. How can distributed memory help reduce round complexity?

2. Lower Bounds in Streaming Models

- Lower bounds of space complexity in the streaming model are reduced to multiparty communication problems:
  1. Element Frenquency F_k.
  2. Matching
  3. Others.

The space complexity of approximating F*_inf

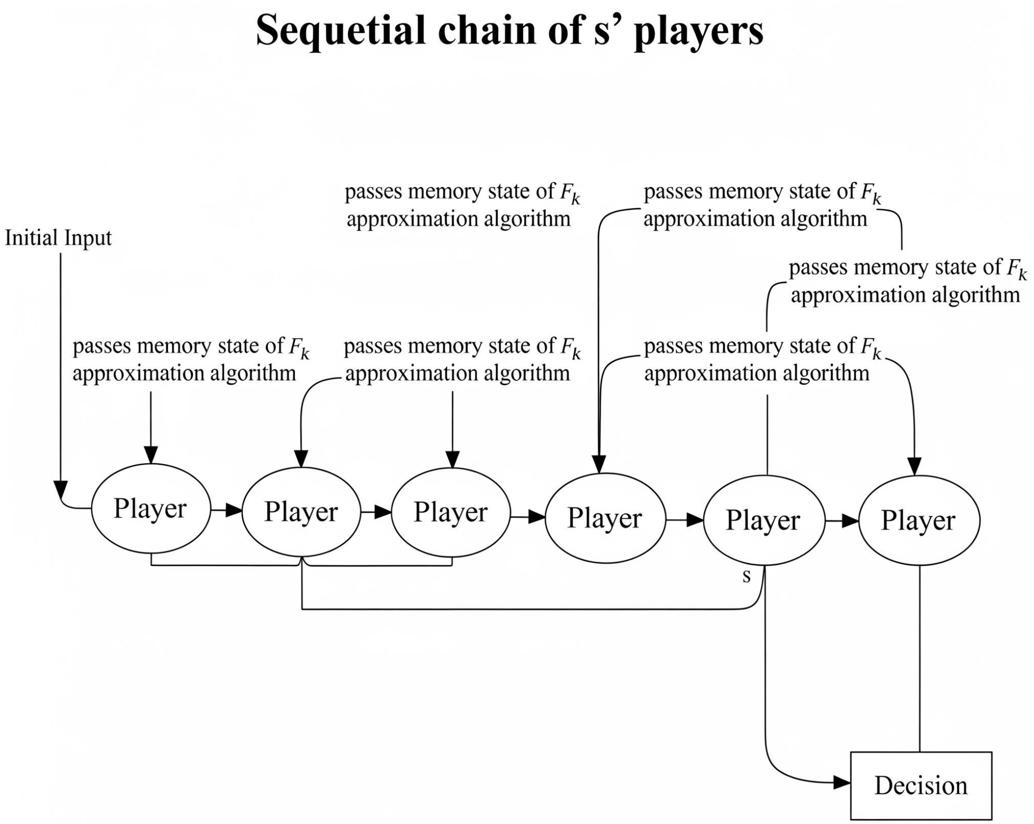
a, b, d, b, e, f : F*_inf = 2



DISJ if the approximate result is less than e.g., 4/3.

Low-Space Streaming Algorithms => Low Communication One-Way Protocols

The space complexity of approximating F_k



$$F_k = \sum_{i=1}^{n} m_i^k$$

m_i: The frequency of the i-th unique value

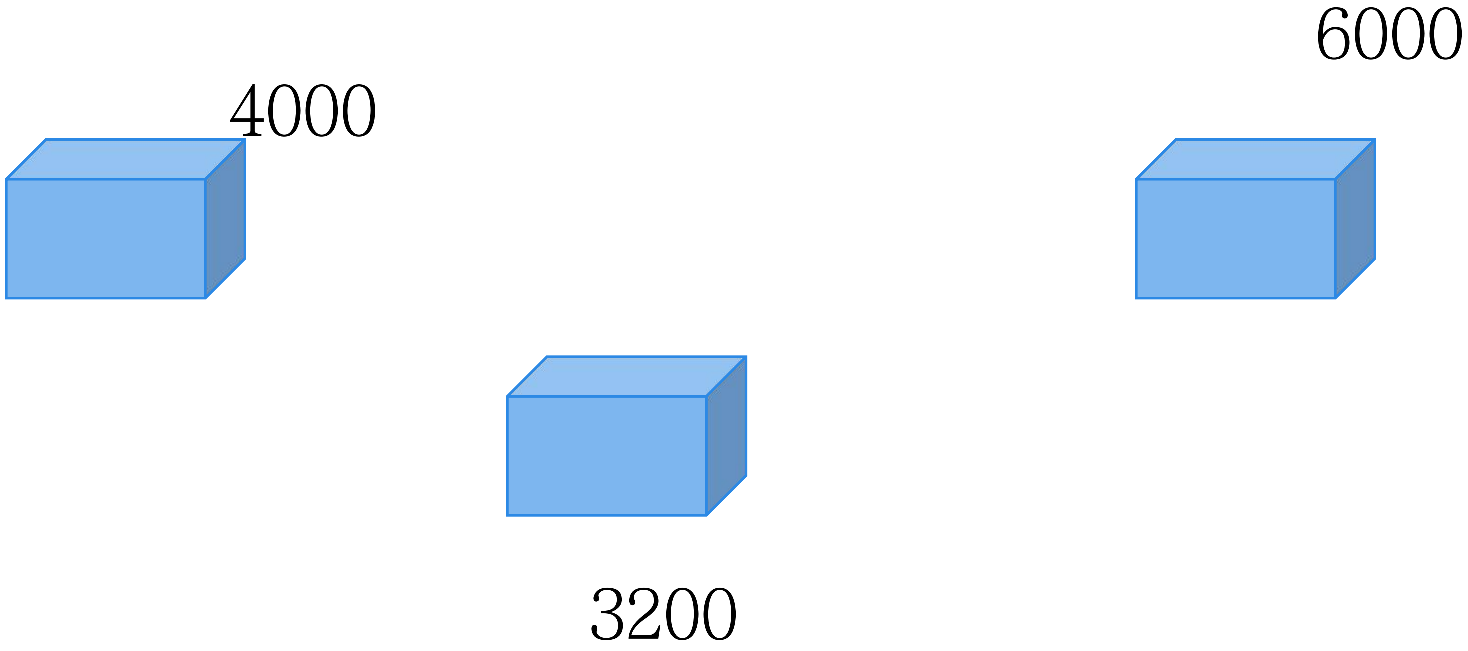
Low-Space Streaming Algorithms => Low Communication Multiparty Communication Protocols

3. Crypotography

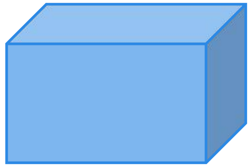
Secure Multiparty Computation (SMPC)

Given k players, p1, p2, ..., pk, each have private data x1, x2, ..., xk. Participants want to compute F(d1, d2, ..., dN) **while keeping their own inputs secret.**

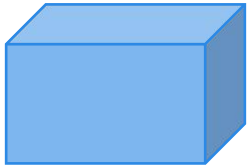
Example: Average Salary



Example: Average Salary

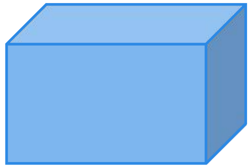


4000 = 1200+ 800+
2000

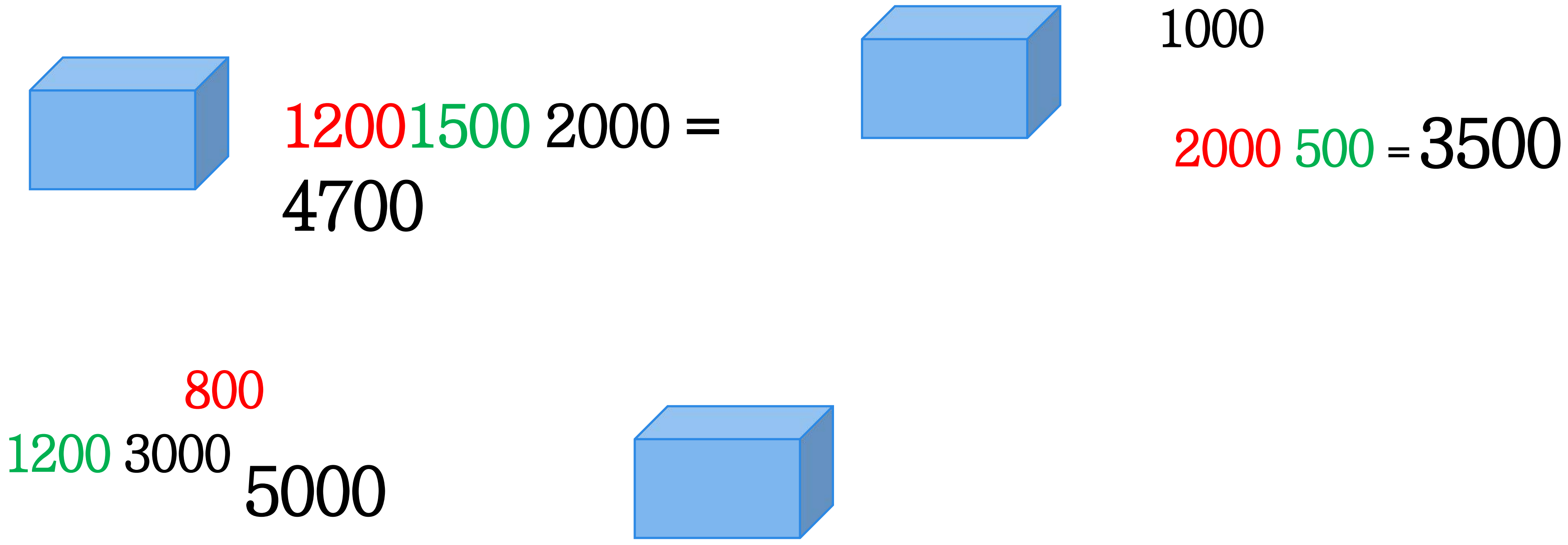


6000 = 1000 + 2000+
3000

3200 = 1200 + 1500 + 500



Example: Average Salary



Benifits of SMPC

- Without the Third Party
- Data Privacy
- Qutuman Safe!

Thanks!